



FÖRSVAR-
UNDERRÄTTELSE-
DOMSTOLEN

Datum
2023-10-20

Diarienummer
Å 49-23
Er referens
Ju2023/01326

Remiss av betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22)

Försvarsunderrättelsesdomstolen har anmodats att yttra sig över kapitel 7, särskilt avsnitt 7.3.5, i betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22). Domstolen får med anledning av vad som framförs i denna del i betänkandet anföra följande.

Nationell säkerhetslagring

Enligt förslaget i betänkandet ska ett beslut om generell och odifferentierad lagringsskyldighet få meddelas om den bedöms vara strängt nödvändig för att bekämpa brottslighet som kan utgöra ett allvarligt hot mot nationell säkerhet som är verkligt och aktuellt eller förutsebart.

Förekomsten av verkliga och aktuella eller förutsebara allvarliga hot mot den nationella säkerheten torde närmast vara ett normaltillstånd. Som exempel kan nämnas att främmande underrättelseverksamhet riktad mot Sverige och svenska intressen i princip alltid innebär ett allvarligt hot mot den nationella säkerheten och det finns sannolikt inte några tidsperioder där sådan verksamhet inte har bedrivits eller kan befarats ha bedrivits. Sett till ordalydelsen framstår det som att de delarna i rekvisitet som regel alltid kommer att vara uppfyllda. Om tanken är att hotet ska vara av mer kvalificerad art bör detta utvecklas inom ramen för den fortsatta beredningen.

Enligt förslaget krävs emellertid även att lagringsskyldigheten bedöms vara absolut nödvändig för att skydda Sveriges säkerhet (se 3 § i förslaget till lag om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet). Begreppet absolut nödvändigt för tankarna till att lagringsskyldigheten måste vara en nödvändig betingelse för att uppnå detta skydd. Med andra ord räcker det alltså inte att lagringsskyldigheten och – framför allt – ett eventuellt senare utlämnande av uppgifterna till de brottsbekämpande myndigheterna kan komma att bidra till att säkerhetshotande brottslighet upptäcks, förhindras eller beivras. En sådan begränsning framstår inte som tillfredställande och är även svår att avgöra inom ramen för en förhandsprövning.

Domstolen kan i anslutning till detta konstatera, i likhet med vad som anförs i det särskilda yttrandet, att EU-domstolens avgöranden bör tolkas på så sätt att det endast är i förhållande till tidsaspekten som EU-domstolen har ställt som krav att lagringsskyldigheten ska vara begränsad till vad som är strängt nödvändigt (jfr p. 131 i SpaceNet- domen).

Av författningskommentaren till bestämmelsen framgår att avsikten är att ge uttryck för den proportionalitetsprincip som är tänkt att gälla vid nationell säkerhetslagring. En sådan proportionalitetsprincip bör dock vara möjlig att formulera på ett tydligare sätt.

Frågorna bör behandlas närmare inom ramen för den fortsatta beredningen.

En effektiv kontroll

Försvarsunderrättsdomstolen delar utredningens bedömning att det bör vara Säkerhetspolisen som gör bedömningen av hoten mot den nationella säkerheten. Det framstår dock som mer tveksamt att Säkerhetspolisen självständigt – om än efter ett sammanträde med ett allmänt ombud och en överklagandemöjlighet – bör få besluta om ett föreläggande om nationell säkerhetslagring.

Enligt domstolens mening torde ett tillståndsförfarande vara att föredra, dvs. att Säkerhetspolisen efter en prövning av ett oberoende organ får tillstånd att förelägga den som är skyldig att lagra uppgifter enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation att lagra de i tillståndet angivna uppgifterna.

Ett sådant system för en oberoende tillståndsgivning skulle kunna byggas upp på ett motsvarande sätt som det som gäller för prövning av tillstånd till signalspaning.

Detta skulle i korthet innebära att Säkerhetspolisen ansöker om tillstånd och i ansökan tydligt redovisar:

- vilket eller vilka allvarliga hot mot den nationella säkerheten som föreligger samt deras verklighet och aktualitet eller förutsebarhet,
- vilka uppgifter som behöver lagras,
- under vilken tid den nationella säkerhetslagringen behövs, samt
- varför det är absolut nödvändigt att uppgifterna lagras för att skydda Sveriges säkerhet.

När ansökan inkommit hålls ett sammanträde där ett ombud deltar. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.

Det oberoende organet prövar därefter om de hot som presenterats är av sådan art att det är proportionerligt med en generell och odifferentierad lagring samt vilka uppgifter som får lagras. Beslutet bör inte kunna överklagas.

Om ansökan beviljas kan Säkerhetspolisen med stöd av beslutet utfärda ett föreläggande.

Val av kontrollorgan

När det gäller vilket organ som ska göra den oberoende prövningen har utredningen föreslagit att ett särskilt beslutsorgan inrättas inom Säkerhets- och integritetsskyddsnämnden, om än i en annan roll än den som domstolen förordar ovan.

Försvarsunderrättsedomstolen anser dock att det finns goda skäl att i den fortsatta beredningen överväga om inte domstolen bör vara det oberoende organ som ansvarar för prövningen i enlighet med vad som anförs ovan. Som utredningen redovisar i betänkandet har domstolen kompetens att bedöma hot mot den nationella säkerheten och att pröva integritetskyddsaspekter. Det finns dessutom en ordning med integritetsskyddsombud som skulle kunna fylla funktionen som offentliga ombud. Vidare har domstolen stor vana att hantera kvalificerat hemliga uppgifter med erforderligt säkerhetsskydd. Med andra ord finns det en befintlig struktur mycket väl lämpad för den aktuella typen av prövningar.

Den principiella invändningen som utredningen för fram mot att Försvarsunderrättsedomstolen bör vara det oberoende organet är, såsom domstolen uppfattat det, att det skulle riskera en sammanblandning av uppgifter och myndigheter på den militära respektive den civila sidan. I den delen får domstolen anföra följande.

Både Försvarets radioanstalt (FRA) och Försvarsunderrättsedomstolen är civila myndigheter. Av de myndigheter som närmare får inrikta signalspaningen är endast en militär (Försvarmakten). Övriga inriktande myndigheter är civila (Regeringskansliet, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten). Att tala om en risk för sammanblandning av uppgifter och myndigheter på den militära respektive den civila sidan framstår därför inte som särskilt relevant och har inte utvecklats närmare i betänkandet. Det kan även noteras att mandatet för försvarsunderrättelseverksamheten anpassades från kartläggning av ”yttre militära hot” till ”yttre hot” 2007, vilket bl.a. innebar att även internationell terrorism och grov gränsöverskridande brottslighet med säkerhetspolitiska konsekvenser kan komma att omfattas av försvarsunderrättelseverksamheten. Som nämns i betänkandet är sambandet mellan inre och yttre säkerhet mer

direkt än tidigare till följd av globaliseringen. Även inre hot mot den nationella säkerheten har således ofta en internationell dimension.

Tillgången till lagrade uppgifter

Inhämtning av information som lagrats med stöd av föreläggandet om nationell säkerhetslagring får enligt förslaget endast avse vissa närmare angivna brott. Prövningen är alltså inte knuten till den hotbedömning som ligger till grund för föreläggandet och ändamålet till att uppgifterna lagras. Detta framstår som tveksamt.

Om de hot mot den nationella säkerheten som motiverar den generella och odifferentierade lagringsskyldigheten t.ex. är främmande underrättelseverksamhet och terrorism, bör inhämtningen av lagrade uppgifter endast vara kopplade till sådana företeelser och brottsmisstankar. Att enbart bedöma inhämtningen i förhållande till en brottskatalog och inte i förhållande till de aktuella hoten som ligger till grund för lagringsskyldigheten framstår som tveksamt och riskerar att komma i konflikt med EU-rätten.

Försvarsunderrättelsesdomstolen har full förståelse för att information rörande nationell säkerhetslagring och bakgrunden till denna är utomordentligt känsliga uppgifter och bör hållas inom en så begränsad krets som möjligt. En fullständig redovisning av hotbilden är således inte lämplig inom ramen för prövningen av tillgång till uppgifter som lagrats med stöd föreläggandet. Det bör dock vara möjligt att på en övergripande nivå redovisa vilken typ av hot som den nationella säkerhetslagringen används för, t.ex. främmande underrättelseverksamhet, terrorism, organiserad brottslighet av systemhotande karaktär etc. Med sådan information kan en domstol eller åklagare pröva om det aktuella fallet har en koppling till hotbilden.

Beslut i detta ärende har fattats av ordföranden Daniel Ström efter föredragning av kanslichefen Mikael Karanikas.

Daniel Ström

Mikael Karanikas